

Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

Claim 1 (currently amended): A method of transferring via a network signed boot files from a server to a PXE client having a pre-OS environment including PXE code, comprising:

installing a PXE client certificate of authenticity in the PXE client;

requesting, by the PXE client using the PXE code via the network that the server, transfer the signed boot files for execution by the PXE client to at least one of create, recreate, modify, expand and enhance an operating system for the PXE client, said requesting occurring after the installation of the client certificate of authenticity in the PXE client;

sending by the PXE client via the network the installed PXE client certificate of authenticity wherein, in response to the receipt of the PXE client certificate of authenticity, the server authenticates the received PXE client certificate of authenticity and wherein, in response to authenticating by the server of the PXE client, sending by the server sends via the network a server certificate of authenticity to the PXE client ~~in response to authenticating by the server of the PXE client;~~

authenticating, by the PXE client, ~~of the server~~ by the received server certificate of authenticity;

requesting, by the authenticated PXE client using the PXE code via the network, ~~that the transfer the signed boot files from~~ authenticated server ~~transfer the boot files to the authenticated PXE client;~~ wherein, in response to receiving the request by the authenticated PXE client, the authenticated server transferring-transfers the signed boot files from the authenticated server to the authenticated PXE client, said signed boot files including a signature corresponding to the PXE client certificate of authenticity or the server certificate of authenticity in response to the requesting by the authenticated PXE client;

authenticating, by the authenticated PXE client, ~~of the transferred~~ signed boot files by the signature of the transferred signed boot files; and

executing by the authenticated PXE client of the authenticated signed boot files thereby creating, recreating, modifying, expanding or enhancing an operating system for the PXE client.

Claim 2 (previously presented): The method of claim 1 wherein PXE clients that have an invalid or revoked certificate are not authenticated or answered by the server.

Claim 3 (previously presented): The method of claim 1 wherein servers that have an invalid or revoked certificate are not acknowledged by the PXE client.

Claim 4 -5 (canceled).

Claim 6 (currently amended): A method of transferring signed boot files from a server to a PXE client having a pre-OS environment including PXE code, comprising:

~~authenticating~~receiving, by the server of the PXE client, ~~the server receiving a request from the PXE client using the PXE code for the transfer of the~~ signed boot files for execution by the PXE client of at least one of create, recreate, modify, expand and enhance an operating system of the PXE client, said request being sent by the client using the PXE code;

receiving, by the server, a PXE client certificate of authenticity, said PXE client certificate of authenticity being installed on the PXE client;

authenticating, by the server, the PXE client by the received PXE client certificate of authenticity;

sending, by the server, a server certificate of authenticity to the authenticated PXE client, wherein in response to receiving said server certificate of authenticity, the authorized PXE

~~authenticating~~client authenticates by the PXE client of the server by the received server certificate of authenticity, and wherein in response to authenticating the server, the

authorized PXE client requests the transfer the signed boot files from authenticated server; and

transferring, by the server, the signed boot files including a signature from the authenticated server to the authenticated PXE client, said signature corresponding to the PXE client certificate of authenticity or the server certificate of authenticity, wherein in response to receiving the PXE client executes the transferred signed boot files, the authenticated PXE client authenticates the transferred signed boot files by the signature of the transferred signed boot files, and wherein in response to authenticating transferred signed boot files, the PXE client executes the authenticated boot files thereby creating, recreating, modifying, expanding or enhancing an operating system of the PXE client.

Claim 7 -8 (canceled).

Claim 9 (previously presented): The method of claim 6 wherein PXE clients that have an invalid or revoked certificate are not authenticated or answered by the server.

Claim 10 (previously presented): The method of claim 6 wherein servers that have an invalid or revoked certificate are not acknowledged by the PXE client.

Claim 11 (previously presented): The method of claim 6 wherein signed boot files received by the PXE client that are incorrectly signed are not executed by the PXE client.

Claim 12 - 40 (canceled).

Claim 41 (currently amended): A system for transferring signed boot files, comprising:

a PXE client including PXE code and an installed PXE client certificate of authenticity, said PXE client including computer executable instructions for:

requesting from a server, by the PXE client using the PXE code, the transfer of signed boot files for execution by the PXE client to at least one of create, recreate, modify, expand and enhance an operating system for the PXE client;

sending, by the PXE client, the installed PXE client certificate of authenticity to the server;

authenticating, by the PXE client, the server by a server certificate of authenticity received from the server;

requesting, by the authenticated PXE client using the PXE code, the transfer the signed boot files from authenticated server;

authenticating, by the authenticated PXE client, the transferred signed boot files by a signature of the transferred signed boot files received from the server, said signature corresponding to the PXE client certificate of authenticity or the server certificate of authenticity; and

executing, by the authenticated PXE client, the authenticated signed boot files thereby creating, recreating, modifying, expanding or enhancing an operating system for the PXE client; and

a server having signed boot files and including computer executable instructions for:

~~-, said server receiving, by the server, a the request from the PXE client using the PXE code that for the server transfer the signed boot files for execution by the PXE client to at least one of create, recreate, modify, expand and enhance an operating system for the PXE client;~~

receiving a PXE client certificate of authenticity, said PXE client certificate of authenticity being installed on the PXE client;

~~software authenticating the PXE client to the server~~ by the received PXE client certificate of authenticity;

~~sending software authenticating the server~~ a server certificate of authenticity to the authenticated to the PXE client; and

~~software transferring the signed boot files~~ including a signature from the authenticated server to the authenticated PXE client, said signature corresponding to the PXE client certificate of authenticity or the server certificate of authenticity in response to the received request wherein the PXE client executes the boot files

~~thereby creating, recreating, modifying, expanding or enhancing an operating system of the PXE client.~~

Claim 42 (canceled).

Claim 43 (currently amended): The method of claim 42, wherein the authenticated PXE client includes an operating system generated from the executed authenticated signed boot files.

Claim 44 (canceled).

Claim 45 (currently amended): A computer readable medium storage for transferring signed boot files via a network ~~boot files~~ from a server to a PXE client having a pre-OS environment including PXE code, comprising instructions for:

~~requesting by the PXE client using the PXE code via the network that the server transfer the signed boot files~~ using the PXE code via the network for execution by the PXE client to at least one of create, recreate, modify, expand and enhance an operating system for the PXE client;

~~sending by the PXE client using the PXE code via the network a previously installed PXE client certificate of authenticity to the server using the PXE code via the network, wherein, in response to the receipt of the PXE client certificate of authenticity, the server authenticates the received PXE client certificate of authenticity and wherein, in response to authenticating of the PXE client by the server, the server sends via the network a server certificate of authenticity to the PXE client;~~

authenticating, by the PXE client, the server by the received server certificate of authenticity;

requesting, by the authenticated PXE client using the PXE code via the network, the transfer the signed boot files from authenticated server to the authenticated PXE client wherein, in response to receiving the request by the authenticated PXE client, the authenticated server transfers the signed boot files to the authenticated PXE client, said

signed boot files including a signature, said signature corresponding to the PXE client certificate of authenticity or the server certificate of authenticity; and
 receiving ~~by the PXE client~~ of the signed boot files from the server;
authenticating the transferred signed boot files by the signature of the transferred signed boot files; and
~~wherein the PXE client~~ executinges the authenticated boot files thereby creating, recreating, modifying, expanding or enhancing an operating system of the PXE client.

Claim 46 (currently amended): A computer readable storage medium for transferring via a network signed boot files from a server to a PXE client having a pre-OS environment including PXE code, comprising instructions for:

receiving ~~by the server~~ a request from the PXE client using the PXE code via the network ~~that the server~~ for the transfer the signed boot files for execution by the PXE client to at least one of create, recreate, modify, expand and enhance an operating system for the PXE client;

receiving ~~by the server~~ via the network a previously installed PXE client certificate of authenticity from the PXE client;

authenticating ~~by the server~~ of the PXE client by the received PXE client certificate of authenticity;

sending a server certificate of authenticity to the authenticated PXE client,
wherein in response to receiving said server certificate of authenticity, the authorized PXE client authenticates the server by the received server certificate of authenticity, and
wherein in response to authenticating the server, the authorized PXE client requests the transfer the signed boot files from authenticated server wherein the signature of the signed boot files corresponds to the PXE client certificate of authenticity or the server certificate of authenticity; and

transferring the signed boot files ~~from the server~~ to the authenticated PXE client
wherein in response to receiving transferred signed boot files, the authenticated PXE client authenticates the transferred signed boot files by the signature of the transferred signed boot files, and wherein in response to authenticating transferred signed boot files,

the authenticated PXE client executes the authenticated boot files thereby creating, recreating, modifying, expanding or enhancing an operating system of the PXE client.

Claim 47-48 (canceled).

Claim 49 (previously presented): The method of claim 1, wherein the PXE code of the PXE client comprises: The Dynamic Host Configuration Protocol (DHCP) for allowing the PXE client to receive an IP address to gain access to the server via the network; a set of application program interfaces (API) for automating the booting of the operating system and other configuration steps on the PXE client; and a standard method of initializing the PXE code in the PXE ROM chip or boot disk of the PXE client.